JOURNAL OF ALGEBRA **82**, 508–515 (1983)

Finite Subgroups of Units of Group Algebras, I*

GERALD J. JANUSZ

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Communicated by Walter Feit

Received January 11, 1982

1. INTRODUCTION

The following question is considered: If G is a finite group and K an algebraic number field, what can be said about the finite subgroups of the unit group of KG which contain G? If the field K is totally real or a totally imaginary quadratic extension of a totally real field, then all the maximal finite groups containing G can be described in terms of certain unitary groups associated with maximal orders containing RG, R the algebraic integers in K. The main result is stated and proved in Section 2. One corollary shows that the trivial units of RG form the unique maximal finite subgroup in RG containing G. The last section is devoted to an analysis of this problem for the case G is a dihedral group and K is the rational field. It is shown in this case that G is contained in a unique maximal finite subgroup of QG and this maximal group is the direct product of groups of order 2 and certain dihedral groups. The uniqueness of the maximal group may be somewhat unexpected but the description as a product of dihedral groups is not suprising since all irreducible representations of a dihedral group have degree one or two and all groups in degree two are known. Other examples and results will be given in a following paper on this problem.

2. GENERAL RESULTS

Let K be an algebraic number field and let $\sigma_1, \ldots, \sigma_{r+2s}$ be the distinct imbeddings of K into the complex field $\mathbb{C}$. Assume the numbering is arranged so that $\sigma_1, \ldots, \sigma_r$ map K into the real field $\mathbb{R}$ and, for each j, σ_{r+j} and σ_{r+j+s} are complex conjugate imbeddings. An automorphism $x \to x^*$ of K is a *complex conjugation* on K if for each index j and for each x in K,

* This work was partially supported by a grant from the National Science Foundation.

0021-8693/83 $3.00

$\sigma_j(x^*)$ is the complex conjugate of $\sigma_j(x)$. If K admits a complex conjugation then, either K is totally real with $*$ the identity, or the fixed field K_0 of $*$ is totally real and K is totally imaginary. An element x in K is *totally positive* if $\sigma_j(x)$ is real and positive for each j. The ring of algebraic integers in K is denoted by R.

The following result must be well known but a proof is included for lack of a reference.

THEOREM 1. *Let K be an algebraic number field which admits a complex conjugation $x \to x^*$.*

(a) *Let n be a fixed positive integer and k some fixed element of K. Then there exist at most a finite number of n-tuples $(\alpha_1, \ldots, \alpha_n)$ of elements of R which satisfy $\alpha_1\alpha_1^* + \cdots + \alpha_n\alpha_n^* = k$.*

(b) *If $\alpha_1, \ldots, \alpha_n$ are elements of R which satisfy $\alpha_1\alpha_1^* + \cdots + \alpha_n\alpha_n^* = 1$ then for some index j, α_j is a root of unity and all other α_i equal 0.*

Proof. The definitions imply that for $\alpha \neq 0$, $\alpha\alpha^*$ is totally positive. Hence it may be assumed that k is totally positive (else no solutions exist). We begin by showing there exist at most a finite number of n-tuples $(\beta_1, \ldots, \beta_n)$ with each β_i a totally positive element of R and $\beta_1 + \cdots + \beta_n = k$.

Consider the map v from K to the $\mathbb{R}$-vector space $\mathbb{R}^r \times \mathbb{C}^s$ defined by

$$v(x) = (\sigma_1(x), \ldots, \sigma_{r+s}(x)).$$

Then v is an additive monomorphism which carries R onto a discrete lattice. For any index j we have $\sigma_j(\beta_1) + \cdots + \sigma_j(\beta_n) = \sigma_j(k)$. The totally positive condition forces $0 \leqslant \sigma_j(\beta_i) \leqslant \sigma_j(k)$. Thus $v(\beta_i)$ lies in a bounded subset. By I.10.2 and I.11.3 of [1] it follows that each β_i lies in a finite subset of R.

In view of this the proof of part (a) is reduced to the proof of the statement: for each totally positive element β in R there exist at most a finite number of α in R which satisfy $\alpha\alpha^* = \beta$. Every such α generates a principal ideal $A = (\alpha)$ which satisfies $AA^* = (\beta)$. But the ideal (β) has only a finite number of factorizations as a product of an ideal and its conjugate. Thus it is sufficient to show there exist only a finite number of elements α in R which satisfy $\alpha\alpha^* = \beta$ and $(\alpha) = A$, A a fixed ideal dividing (β). If α_1 is another element which satisfies these conditions then $(\alpha) = (\alpha_1)$ so $\alpha_1 = \mu\alpha$. μ a unit of R. Since $\alpha_1\alpha_1^* = \alpha\alpha^*$, it follows that $\mu\mu^* = 1$. Now each $\sigma_j(\mu)$ has absolute value 1 so $v(\mu)$ lies in a bounded subset of $\mathbb{R}^r \times \mathbb{C}^s$. Thus only a finite number of μ are possible; this proves part (a).

Now suppose $\alpha_1 \neq 0$ and $\alpha_1\alpha_1^* + \cdots + \alpha_n\alpha_n^* = 1$. If some $\alpha_j \neq 0$ for $j \neq 1$ then, for all i,

$$0 < \sigma_i(\alpha_1\alpha_1^*) < 1.$$

Thus we obtain

$$0 < N_{K/Q}(\alpha_1 \alpha_1^*) = \sigma_1(\alpha_1 \alpha_1^*) \cdots \sigma_{r+2s}(\alpha_1 \alpha_1^*) < 1.$$

However, when α_1 is in R, $N_{K/Q}(\alpha_1 \alpha_1^*)$ is an integer and cannot lie strictly between 0 and 1. It follows that only one α is non-zero and it satisfies $\alpha\alpha^* = 1$. By part (a) the set of such α is finite and is a group under multiplication. Thus α is a root of unity and part (b) is proved.

Let K be an algebraic number field which admits a complex conjugation $x \to x^*$ and let G be a finite group of order n. Define an involution J on KG by the rule

$$J\left(\sum \alpha(g)\, g\right) = \sum \alpha(g)^* g^{-1},$$

where $\alpha(g)$ is in K and the sum is over all g in G. This map is clearly additive and one can show $J(xy) = J(y)\,J(x)$ for all x, y in KG. Since J^2 is the identity, J is an involution. For any subring Λ of KG let

$$U_J(\Lambda) = \{\lambda \in \Lambda : \lambda J(\lambda) = 1\}.$$

It is easily verified that $U_J(\Lambda)$ is a (multiplicative) group. These groups are of special interest in our main problem. As before R denotes the integers in K. The unit group of KG is denoted by $KG^\times$.

THEOREM 2. *If Λ is an R-order in KG which contains RG, then $U_J(\Lambda)$ is a finite group containing G. As Λ ranges over all maximal R-orders containing RG, the groups $U_J(\Lambda)$ range over all maximal finite subgroups of $KG^\times$ which contain G.*

Proof. Let Λ be an R-order which contains RG. Then certainly $G \subseteq U_J(\Lambda)$. We show $U_J(\Lambda)$ is finite. By Theorem 41.1 of [2] we have

$$RG \subseteq \Lambda \subseteq n^{-1}RG.$$

If λ is an element in $U_J(\Lambda)$ then there are elements $\alpha(g)$ in R such that

$$n\lambda = \sum \alpha(g)\, g.$$

The equation $\lambda J(\lambda) = 1$ implies

$$n^2 = \sum \alpha(g)\, \alpha(g)^*.$$

By part (a) of Theorem 1 there exist only a finite number of n-tuples $(\alpha(g))$ and so only a finite number of possible λ. Hence $U_J(\Lambda)$ is finite.

Now let H be a finite subgroup of $KG^\times$ which contains G. Let Λ be the ring generated by R and the elements of H. Then Λ contains RG and Λ is an R-order. In order to prove the theorem, it is enough to show that $H \subseteq U_J(\Lambda)$; in other words it is enough to show $J(h) = h^{-1}$ for each h in H.

We begin the proof of this fact. View H as an abstract group and consider the group algebra KH and its involution which invertes elements of H and induces the conjugation on K. The inclusion of H into $KG^\times$ induces a K-algebra epimorphism $f: KH \to KG$. As a first step it is necessary to show that kernel f is J_H-invariant. Since every nonzero ideal is a sum of simple ideals, it is sufficient to show each simple ideal is J_H-invariant. A simple ideal M has the form $M = KHe$ for a central idempotent element $e = \sum \beta(g)g$. Some coefficient $\beta(g_1)$ is nonzero and so $eJ_H(e)$ is non-zero because the coefficient of the identity is the sum of the totally positive (or zero) elements $\beta(g)\beta(g)^*$ at least one of which is non-zero. But now $J_H(e)$ is also a central idempotent and is either equal to e or is orthogonal to e. We have just seen it is not the latter so $e = J_H(e)$ and $M = J_H(M)$ follows. Hence $J_H(\ker f) = \ker f$. This means J_H induces an involution $J_0(f(x)) = f(J_H(x))$ for x in KH. The map f was induced by the inclusion of H into KG so we find for all h in H that

$$J_0(h) = fJ_H(h) = f(h^{-1}) = h^{-1}.$$

So in particular KG supports the two involutions J and J_0 both of which invert the elements of G (as $G \subseteq H$) and induce conjugation on K. In particular $J = J_0$ and so J inverts H as required to complete the proof.

COROLLARY. *There are only a finite number of finite subgroups of $KG^\times$ which contain G.*

Proof. It is sufficient to prove there exist only a finite number of maximal finite subgroups of $KG^\times$ containing G. This will follow from the theorem if we show there exist only a finite number of maximal orders containing RG. Every such maximal order lies between RG and $n^{-1}RG$. Since RG has finite index in $n^{-1}RG$, only a finite number of subgroups and hence only a finite number of orders lie between RG and $n^{-1}RG$.

It is well-known result that if G is an abelian group, then every unit of RG which has finite order is a root of unity in R times an element of G. It is also well known that if G is non-abelian, RG may contain elements of finite order not of this form. Our methods give the following generalization of the abelian case.

COROLLARY. *For any finite group G, there is a unique maximal finite subgroup of the units of RG which contains G. It is the group of all units of the form μg with μ a root of unity in R and g in G.*

Proof. The unique maximal finite subgroup of the units of RG containing G is $U_J(RG)$ by the theorem. Let $\lambda = \sum \alpha(g)g$ be an element of this group. Then each coefficient $\alpha(g)$ lies in R. The equation $\lambda J(\lambda) = 1$ implies

$$1 = \sum \alpha(g)\,\alpha(g)^*.$$

The corollary now follows from Theorem 1b.

3. Dihedral Groups

Let Q denote the rational field and D a dihedral group of order $2n$. We shall prove that D is contained in a unique maximal finite subgroup of QD and also describe this maximal group explicitly.

Let $D = \langle a, b: a^n = b^2 = 1, bab = a^{-1}\rangle$. The description of QD will use the following crossed product algebras. Let ζ be a root of unity of order $m \geqslant 3$ and let τ be the automorphism of $Q(\zeta)$ which inverts ζ. Then τ has order 2. Let $A(\zeta)$ denote the algebra

$$A(\zeta) = (Q(\zeta), \tau, 1) = Q(\zeta) + Q(\zeta)\,u_\tau,$$

where $u_\tau^2 = 1$ and $u_\tau x = \tau(x)\,u_\tau$ for x in $Q(\zeta)$. Then $A(\zeta)$ is isomorphic to a 2×2 matrix ring over the field $Q(\zeta + \zeta^{-1})$.

Finally let k denote the index of the commutator subgroup of D; $k = 2$ if n is odd and $k = 4$ if n is even.

Theorem 3. *The decomposition of QD into a direct sum of simple rings is described as follows: There are k summands isomorphic to Q. For each divisor m of n with $m \geqslant 3$ let ζ_m denote some primitive mth root of unity. There is one simple summand of QD isomorphic to $A(\zeta_m)$. The total number of simple summands equals the number of divisors of n plus $\frac{1}{2}k$.*

Proof. The group D has k distinct linear characters all of which have their values in Q. Hence QD has k summands isomorphic to Q and this accounts for all commutative summands. Suppose m is a divisor of n with $m \geqslant 3$. Then the group $\langle \zeta_m, u_\tau\rangle$ in $A(\zeta_m)$ is an epimorphic image of D under the correspondence $a \to \zeta_m$, $b \to u_\tau$. Since $A(\zeta_m)$ is generated over Q by ζ_m and u_τ it follows that QD maps onto $A(\zeta_m)$ and so $A(\zeta_m)$ is one of the simple summands of QD. No two of these summands are isomorphic since we select only one ζ_m for each divisor m. To show that all summands have been

counted, we compute dimensions over Q. The Euler function ϕ has the property $\sum \phi(m) = n$ if m ranges over all divisors of n. Thus the sum

$$\sum_{m \geqslant 3} (A(\zeta_m) : Q) = \sum_{m \geqslant 3} 2\phi(m) = 2n - k.$$

It follows that all summands have been counted.

In order to locate the maximal finite subgroups of $QD^\times$ containing D, it is sufficient to obtain the maximal Z-orders in QD and then determine their unitary groups U_J. A maximal order in the direct sum of simple rings is a direct of maximal orders in the summands. Hence we work in the summands $A(\zeta)$ before stating the final result.

Let $\Lambda = Z[\zeta] + Z[\zeta]u$. Then Λ is the projection of ZD into $A(\zeta)$ and it is necessary to find the maximal orders containing Λ. There is one case where the work has been done already. Assume that the order m of ζ is divisible by two odd primes or by an odd prime and by 4. Then $Z[\zeta]$ is unramified over $Z[\zeta + \zeta^{-1}]$ and the theorem of Auslander–Goldman–Rim [40.14, 2] implies that Λ is already a maximal order in $A(\zeta)$. Hence there is a unique maximal finite subgroup of $A(\zeta)^\times$ containing $\langle \zeta, u_\tau \rangle$ and it is $U_J(\Lambda)$. Let $\lambda = x + yu_\tau$ be an element of this group, with x, y in $Z[\zeta]$. Then

$$\begin{aligned} 1 = \lambda J(\lambda) &= (x + yu_\tau)(x^* + u_\tau y^*) \\ &= xx^* + yy^* + 2xyu_\tau. \end{aligned}$$

It follows from Theorem 1b that one of x or y is a root of unity and the other is 0. If $W(\zeta)$ denotes the group of roots of unity in $Z[\zeta]$, then $U_J(\Lambda) = \langle W(\zeta), u_\tau \rangle$. Note that $W(\zeta)$ is cyclic with generator ζ if the order of ζ is even and with generator $-\zeta$ if the order of ζ is odd.

Now we turn to the remaining case; namely, we assume the order of ζ is a prime power or twice an odd prime power. In the latter case ζ^2 has prime power order and $Q(\zeta) = Q(\zeta^2)$ so we shall assume ζ has prime power order $p^t \geqslant 3$. In order to simplify the notations let $S = Z[\zeta]$ and $R = Z[\zeta + \zeta^{-1}]$. The trace map is $T(x) = x + x^* = x + \tau(x)$ for x in $Q(\zeta)$. If $f = 1 + u_\tau$ then $fxf = T(x)f$ and $u_\tau f = f$.

Suppose Γ is a maximal order in $A(\zeta)$ containing Λ. We have then $\Lambda f \subseteq \Gamma f \subseteq A(\zeta)f$. From the descriptions of Λ and $A(\zeta)$ one sees $\Lambda f = Sf$ and $A(\zeta)f = Q(\zeta)f$. It follows that $\Gamma f = Mf$ for some τ-invariant fractional S-ideal M in $Q(\zeta)$. The *left order* of Mf is $\{\alpha \in A : \alpha Mf \subseteq Mf\}$. This is an order containing Γ so it must equal Γ by maximality. The left order of Mf can be described using the different Δ of the extension $Q(\zeta)/Q(\zeta + \zeta^{-1})$. We claim that $\Gamma = MfM^{-1}\Delta^{-1}$. To verify this we first note

$$(MfM^{-1}\Delta^{-1})\, Mf = Mf\Delta^{-1}f = T(\Delta^{-1})\, Mf \subseteq Mf.$$

Thus $MfM^{-1}\Delta^{-1}$ is contained in Γ. Next it is clear from the inclusion $\Gamma Mf \subseteq Mf$ that $MfM^{-1}\Delta^{-1}$ is a left ideal of Γ. Suppose M is a free R-module on a basis m_1, m_2. Then its dual basis y_1, y_2 lies in $M^{-1}\Delta^{-1}$ and so $m_1 f y_1 + m_2 f y_2 = w$ is an element of the left ideal. However, it is not difficult to show that w is the identity element. Hence $\Gamma = MfM^{-1}\Delta^{-1}$ in this case. If M is not necessarily free, we first localize to make it free. Then equality holds at every localization and hence global equality holds. This gives a description of all maximal orders containing Λ. Now we show there are at most two distinct such orders. If X is any fractional R-ideal in $Q(\zeta + \zeta^{-1})$ then $(XM)f = MfX$ and so Mf and XMf have the same left order. This fact is exploited by using facts about ideals of S. Let $\pi = \zeta - \zeta^{-1}$ so π^2 is in R. Then $\pi S = (\pi)$ is a prime ideal and equals the different Δ. Moreover (π) is the only ramified prime of S over R and so any $\langle\tau\rangle$-invariant fractional ideal of S has the form XS or $X(\pi)$ with X some fractional R-ideal in $Q(\zeta + \zeta^{-1})$. Hence the ideal M may be taken as S or (π). Since π^2 is in R this means the only maximal orders containing Λ are $\Gamma_1 = Sf S\pi^{-1}$ and $\Gamma_2 = \pi^{-1}Sf S$. Since $J(\pi) = -\pi$, it follows that $J(\Gamma_1) = \Gamma_2$ and $J(\Gamma_2) = \Gamma_1$. The two groups $U_J(\Gamma_i)$ are J-invariant; we find $U_J(\Gamma_i)$ lies in $\Gamma_1 \cap \Gamma_2$. Thus

$$U_J(\Gamma_1) = U_J(\Gamma_1 \cap \Gamma_2) = U_J(\Gamma_2).$$

Once again there is a unique maximal finite group containing $\langle \zeta, u_\tau \rangle$. Let $\gamma = (x + yy_\tau)\pi^{-1}$ be an element of $U_J(\Gamma_i)$ with x, y in S. Then

$$1 = \gamma J(\gamma) = (xx^* + yy^* + 2xyu_\tau)(-\pi^{-2}).$$

Just as in the previous case either $x = 0$ or $y = 0$ which means that either γ or γu_τ is an element of finite order in $Q(\zeta)$. Thus $U_J(\Gamma_i) = \langle W(\zeta), u_\tau \rangle$ with $W(\zeta)$ the roots of unity in $Q(\zeta)$.

We now may collect the results of these computations.

THEOREM 4. *Let D be a dihedral group of order $2n$. There is a unique maximal finite subgroup of $QD^\times$ which contains D. It is a direct product of k copies of the group of order 2 ($k = 2$ if n is odd, $k = 4$ if n is even) and one copy of each group $\langle W(\zeta_m), u_\tau \rangle$, where ζ_m is a primitive mth root of unity, m is a divisor of n with $m \geqslant 3$, $W(\zeta_m)$ is the group of roots of unity in $Q(\zeta_m)$ and u_τ is an element of order 2 which inverts ζ_m.*

Remarks. 1. The orders Γ_1 and Γ_2 which appear in the proof are each isomorphic to the ring of 2×2 matrices over R. However, the orders are not equal in general.

2. A generalization of the methods used in this section will be applied in some other cases in a forthcoming work.

REFERENCES

1. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York/London, 1973.
2. I. REINER, "Maximal Orders," Academic Press, New York/London, 1975.